

A File Locker System

Course No: CSE4116

Course Name: Computer and Network Security Laboratory

Submitted To:

Dr. Kazi Md. Rokibul Alam

Professor

Dept of Computer Science and Engineering

Khulna University of Engineering & Technology, Khulna-9203

Sheikh Imran Hossain

Assistant Professor

Dept of Computer Science and Engineering

Khulna University of Engineering & Technology, Khulna-9203

Submitted By:

Mohaimen Hasan

Roll: 1507040

Section: A

Dept of Computer Science and Engineering

Khulna University of Engineering & Technology, Khulna-9203

Objective:

- The main objective of this project is to learn encryption and decryption of files to maintain security..
- Know about different types of encryption and decryption mechanism.
- Know about how the encryption decryption algorithm works.
- Know how we can ensure the security of our file using encryption decryption algorithm.

Introduction:

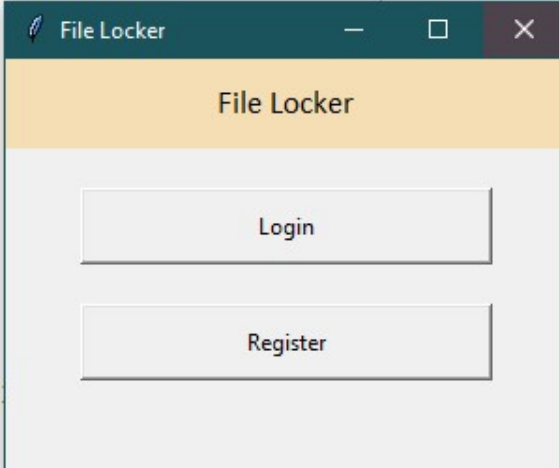
Computer security is important, primarily to keep information protected. The increased use of computer and communications system by industry has increased the risk of theft of proprietary information although these threats may require a variety of counter measures. Encryption is a primary method of protecting valuable electronic information. Encryption is the process of encoding a message in such a way as to hide its contents. Modern cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secrets called keys. A cryptography key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without the knowledge of the key. Terms used in cryptography are as follows:

- Plain text: original message is known as plain text.
- Cipher text: coded message is known as cipher text.
- Encryption: the process of converting the plain text to cipher text is known as encryption.
- Decryption: the process of restoring the plain text from the cipher text is known as decryption.

There are different methods to encrypt and decrypt files. Among them I used RSA encryption decryption mechanism to encrypt and decrypt files.

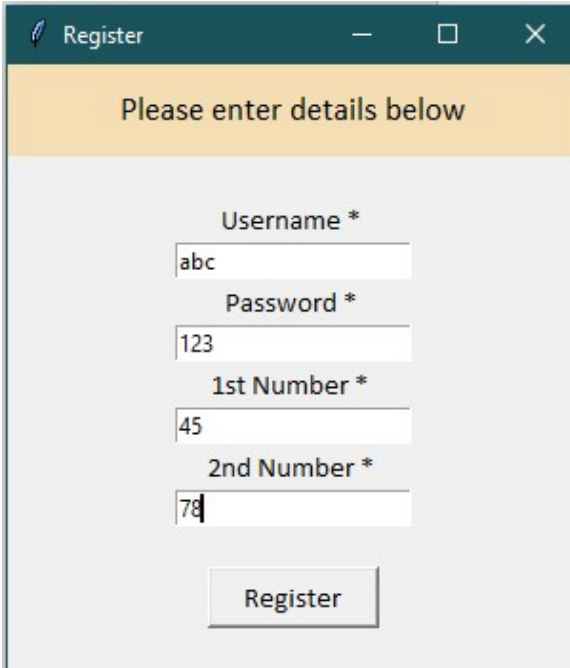
Project Description:

First of all, there is a window for register and login. A user must login to go to the next window and continue encryption or decryption.



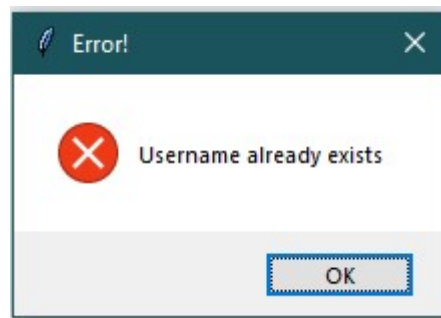
The image shows a window titled "File Locker" with a dark teal header bar containing a feather icon, the title, and standard window controls. Below the header is a light orange bar with the text "File Locker". The main area is light gray and contains two white buttons with black text: "Login" and "Register".

In the Register window user must give a username, password and two random numbers. These numbers are used to calculate public keys and private key for that user. These keys are fixed for that user. In every encryption or decryption process only these keys will be used for that user. There is a seldom chance that keys of two users will be same.



The image shows a window titled "Register" with a dark teal header bar containing a feather icon, the title, and standard window controls. Below the header is a light orange bar with the text "Please enter details below". The main area is light gray and contains four input fields with labels: "Username *" (containing "abc"), "Password *" (containing "123"), "1st Number *" (containing "45"), and "2nd Number *" (containing "78"). Below the input fields is a white button with black text: "Register".

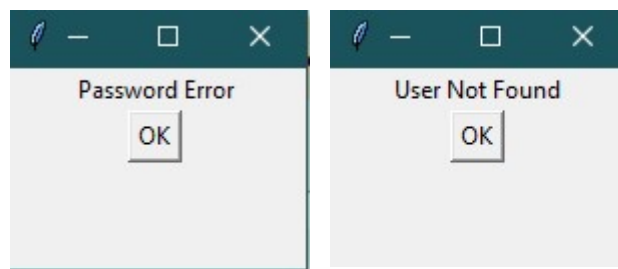
If the username already exists, an error window will occur showing unsuccessful registration.



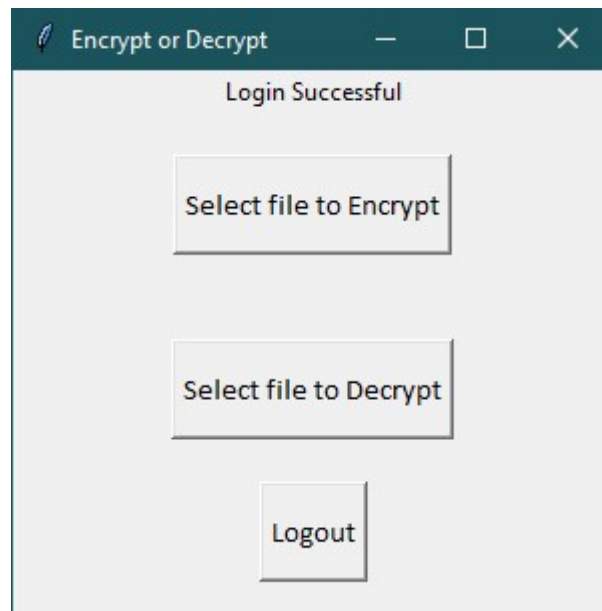
After successful registration, a window showing successful registration will occur.



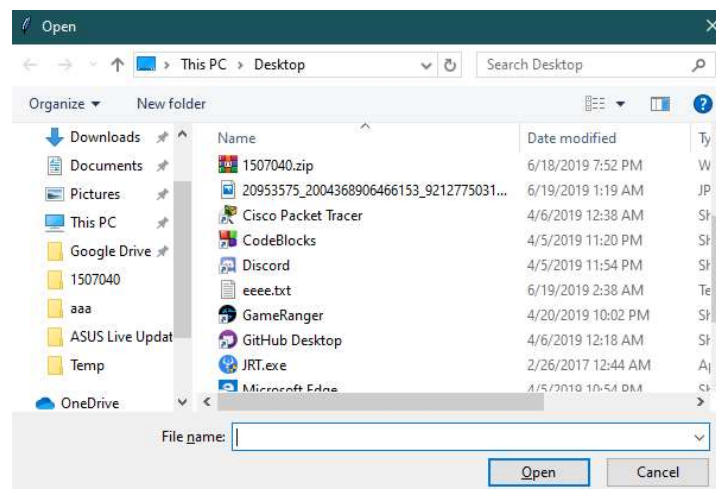
In the login window, user must give correct username with correct password in the given fields. For specific action there are specific windows.



After successful login Encrypt or Decrypt window would come. There are three buttons in this window.



First button would open a file dialog to choose file for encryption. The second button will also open a file dialog but for decryption. And the last button is for logout. By clicking logout user will go to the home window.



If the encryption is complete encryption successful message will pop-up. The encryption is done by the keys that were generated in registration process for that user. Decryption process is done using the same procedure as encryption.

Conclusion:

So, the system can easily encrypt and decrypt any type of file in a short time. The original file is deleted instantly after encryption. These will prevent attacker from accessing sensitive file information. Every user has different public and public key. So, one user cannot decrypt others encrypted file.